REMARKS

STATUS OF THE CLAIMS

Claims 6, 8, and 11-13 are pending in the application.

Claims 6, 8, and 11-13 are rejected.

Claim 6, 8 and 11 are amended, new claims 21-23 are added, and, thus, claims 6, 8, 11-13, and 21-23 remain pending for reconsideration, which is respectfully requested.

No new matter has been added in this Amendment. The foregoing rejections are hereby traversed.

CLAIM REJECTIONS – 35 U.S.C. §102 AND §103

Claims 6, 8 and 11 were rejected under 35 U.S.C. 102(e) as being anticipated by Keathley et al. (U.S. Patent No. 6,247,129 B1).

Claims 12 and 13 were rejected under 35 U.S.C. 103(a) as being unpatentable over Keathley (U.S. Patent No. 6,247,129 B1).

The independent claims are 6, 8, and 11, which are anticipatorily rejected by Keathley.

The independent claims 6, 8, and 11, using claim 6 as an example, are amended for clarity, as follows:

> 6. (CURRENTLY AMENDED) A process of user authentication in a client computing apparatus, comprising:
>
> executing, in the client computing apparatus, a web browser processingthat processes a protected web page received from the-network;
>
> storing on an integrated circuit card a certificate to access the protected web page received in the client computing apparatus and characteristic identifying information of a user associated with the received protected web page;
>
> reading by an integrated circuit card reader the integrated circuit, in response to the receipt of the protected web page by the web browser of the client computing apparatus;
>
> comparing identifying information input by the user with the characteristic identifying information of the user stored in the integrated circuit card; and
>
> in response to the comparing, providing the certificate stored on the integrated circuit card to the web browser of the client computing apparatus to access the received protected web page.

Support for the claim amendments can be found, for example, on page 14, lines 7-9 and page 15, lines 20-23, and FIGS. 12-13, of the present Application.

Keathley discloses a system for network-based electronic commerce employing an integrated circuit card, where the integrated circuit card (ICC) 234 generates an authorization request cryptogram (ARQC) which is used by issuer server 112 to authenticate the card (column 5, lines 30-32). In particular, the Examiner, in page 3 of the Office Action, appears to primarily rely on Keathley, column 6, lines 35-67 and Keathley column 6, lines 43-45, disclose, "[Cardholder Accessed Device] CAD 102 retrieves this URL [from the ICC 234] and accesses the identified network address to retrieve and display images identifying the card issuer and payment brand." However, in contrast to Keathley, the claimed present invention provides, "storing on an integrated circuit card *a certificate to access the protected web page received in the client computing apparatus* and characteristic identifying information of a user associated with the received protected web page" (e.g., amended independent claim 6). Therefore, Keathley discloses that the ICC 234 stores a URL that is used by the card access device (CAD) 102 to retrieve from the network a web page. In contrast, in the claimed present invention the ICC stores "*a certificate* to *access the protected web page received in the client computing apparatus*."

Further, Keathley, column 6, lines 63-67, and FIG. 4, disclose,

> Step 422 begins an on-line authorization procedure where issuer 112 may verify the authenticity of integrated circuit card 234. CAD 102 requests generation of an authorization request cryptogram (ARQC) if PIN entry was successful, or an application authorization cryptogram (ACC) if PIN entry was not successful.

Therefore, in Keathley, the ICC 234 serves as a *cryptographic processor*, to protect integrity and authenticity of *a transaction transmitted* over the network and for *authentication of the ICC 234 by the issuer 112* (i.e., at FIG. 4, operation 422, the ICC 234 generates an application cryptogram, see column 1, lines 36-38, column 5, lines 28-32). More particularly, Keathley, as shown in FIG. 1, uses the ICC 234 for on-card symmetric cryptographic processing for protecting *electronic commerce transaction transmissions* and for *authentication of the ICC card 234* between the client computer (card access device 102) and network servers, such as merchant server 104, payment gateway 108, acquire (bank) server 109, and issuer server 112. See, Keathley, Abstract, and column 5, lines 28-32. In contrast to Keathley, the claimed present invention provides, "in response to the comparing, providing the *certificate stored on the integrated circuit card* to the *web browser of the client*

7

computing apparatus to access the received protected web page" (e.g., claim 6).

In other words, in Keathley, FIG. 4, at operation 422, the authorization request cryptogram (ARQC) is not used by the card access device (CAD) 102 to access a received protected web page, but in Keathley, the ARQC generated by the ICC 234 is transmitted by the card access device 102 over the network as part of a transaction, such as to formulate a purchase request, and the ARQC is used by the issuer 112 to authenticate the card. In other words, a Keathly generated cryptogram by the ICC cannot be used to access a protected web page, because the cryptogram is an encryption process whereas the claimed present invention's, "*a certificate to access the protected web page* received in the client computing apparatus," is for an authentication process at the client computing apparatus *to access a received web page* (see, page 14, lines 7-9 and page 15, lines 20-23, and FIGS. 12-13, of the present Application).

Regarding Keathley's cardholder certificate stored on the ICC 234, the card access device 102 does not use the cardholder certificate to access a web page received by the card access device 102. But Keathley's card access device 102, uses the cardholder certificate to protect a *transaction transmitted* over the network and for the issuer 112 to *authenticate the ICC 234*, because Keathley's "cardholder certificates function as electronic representation of a payment card" (column 4, lines 50-54). Therefore, Keathley's cardholder certificate also differs from the claimed present invention's, "*a certificate to access the protected web page* received in the client computing apparatus" (e.g., claim 6).

Also, Keathley, column 5, lines 53-57 and FIG. 4, which is relied upon by the Examiner in page 6 of the Office Action, expressly discloses, "prior to processing of the transaction, at step 402, the cardholder shops, e.g., by browsing through the merchant's web site. CAD 102 may be equipped with an HTTP-compatible browser to facilitate viewing catalog information stored on merchant server 104." Therefore, as disclosed in Keathley, column 5, lines 53-57, Keathley does not disclose or suggest the claimed present invention's, "storing on an integrated circuit card *a certificate to access the protected web page received in the client computing apparatus*."

Therefore, neither Keathley's cryptographic processor function of the integrated circuit card (FIG. 4, operation 422, column 4, line 51 to column 8, line 34), nor Keathley's cardholder certificate (column 4, lines 50-51), disclose or suggest the claimed present invention's, "storing on an integrated circuit card *a certificate to access the protected web page received in the client computing apparatus*, ... and in response to the comparing, *providing the certificate*

8

stored on the integrated circuit card *to the web browser of the client computing apparatus to access the received protected web page*" (e.g., independent claim 6), and the claimed present invention as recited in independent claims 6, 8 and 11 is patentably distinguishing over Keathley.

DEPENDENT CLAIMS 12-13 AND NEW DEPENDENT CLAIMS 21-22

Further, regarding the Examiner's obviousness rejection of dependent claims 12-13 over Keathley, the Examiner on page 6 asserts that Keathley discloses displaying a link within a browser to a secure merchant server for initiating a purchase request (column 5, lines 53-63). Then, the Examiner on page 6 asserts, "It would have been obvious ... to display selectable names of protected applications as protected web pages, if a result of comparing user identifying information is matching, in order to further secure the system ..."

However, in contrast to Keathley, the claimed present invention, as recited in dependent claim 12 provides, "displaying ... *selectable names of protected applications as protected web pages* ... and ... *providing one of a plurality of certificates stored on the integrated circuit card and corresponding to a selected one of the protected applications by the user* to the web browser *to access the selected protected application*." In other words, Keathley does not disclose or suggest anywhere prompting the user to *select* authentication information *to access a protected web page*, and Keathley's disclosure concerning displaying a link to a secure merchant server relates to protecting *electronic commerce transaction transmissions* between the client computer (card access device 102) and network servers, such as merchant server 104, payment gateway 108, Acquire (bank) server 109, and issuer server 112, via the ICC 234 generating cryptograms, but Keathley is silent on generating different cryptograms corresponding to different issuers 112.

In particular, Keathley, column 5, lines 53-57, which is relied upon by the Examiner in page 6 of the Office Action, expressly discloses, "prior to processing of the transaction, at step 402, the cardholder shops, e.g., by browsing through the merchant's web site. CAD 102 may be equipped with an HTTP-compatible browser to facilitate viewing catalog information stored on merchant server 104." Therefore, as disclosed in Keathley, column 5, lines 53-57, Keathley does not disclose or suggest the claimed present invention's dependent claim 12, "displaying ... *selectable names of protected applications as protected web pages*, ... and ... *providing one of a plurality of certificates stored on the integrated circuit card and corresponding to a selected one of the protected applications by the user* to the web browser *to access the selected protected application*."

9

A benefit of the claimed present invention is to allow the user manage multiple certificates corresponding to multiple protected web pages, which does not coincide with the Examiner's alleged obviousness motivation that Keathley displays a link within a browser to a secure merchant server for initiating a purchase request. In other words, according to the present invention, when the web browser requests and receives an encrypted web page to be displayed, the web browser requests a certificate to decrypt the received encrypted web page. The integrated circuit card of the present invention manages and provides certificates corresponding to encrypted web site applications that are sent to/received by the web browser and require decryption by the web browser.

Therefore, Keathley cannot provide suggestion, or motivation to be modified, to achieve the claimed present invention as recited in dependent claim 12.

New dependent claims 21 and 22 depending from independent claim 6 are along the lines of dependent claims 12 and 13, and are patentably distinguishing over Keathley as discussed above. In particular, in contrast to Keathley, the claimed present invention as recited in new dependent claim 21 provides:

> 21. (NEW) The process of claim 6, further comprising:
>
> *displaying*, by the integrated circuit, on a display unit *selectable names of protected applications, as protected web pages received in the client computing apparatus*, if a result of the comparing of the user identifying information is matching; and
>
> the providing of the certificate stored on the integrated circuit comprises *providing to the web browser of the client computing apparatus, one of a plurality of certificates stored on the integrated circuit card that correspond to a selected one of the protected applications by the user* to access by the client computing apparatus the selected protected application (emphasis added).

<u>NEW DEPENDENT CLAIM 23</u>

In contrast to Keathley, the present invention as recited in new dependent claim 23 provides:

> 23.   (NEW) The process of claim 21, further comprising:
>
> storing, in the integrated circuit card, **an application identifier identifying a protected application to display a selectable name of the protected application**, and a user identifier and password **as the characteristic identifying information of the user associated with the protected applications as the protected web pages received in the client computing apparatus**.

Keathley fails to disclose or suggest the claimed present invention's, "**an application identifier identifying a protected application to display a selectable name of the protected application**," as described in the present Application with reference to FIGS. 12 and 13. Support for new claim 23 can be found, for example, in page 15, lines 4-9 and FIG. 14 of the present Application.

CONCLUSION

In view of the claims amendments and remarks, withdrawal of the rejection of pending claims and allowance of pending claims is respectfully requested.

If there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

Respectfully submitted,
STAAS & HALSEY LLP

Date: ___12/13/2004___   By: _____

Mehdi D. Sheikerz
Registration No. 41,307

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501